

## Re: Tracking User activity on 4.3.3

**Source:** <http://unix.derkeiler.com/Mailing-Lists/AIX-L/2005-11/0059.html>

---

**From:** Yves Dorfsman (yves\_at\_ZIOUP.COM)

**Date:** 11/10/05

Date: Wed, 9 Nov 2005 20:24:53 -0700  
To: aix-l@Princeton.EDU

"rootsh" is probably the least bad solution for this.

I am sure you understand that by giving root privileges to a user, you give that user the power to hide its actions, and undo everything you do, including whatever you do to track its actions.

On Wed, 9 Nov 2005, Vipin Khushu-Suse wrote:

> *Greetings All:*

>

> *I'll setting up a new user (other than root) with root authority. And yes, the admonition against this practice is duly noted by yours truly.*

>

> *In order to keep a close watch on things, I need to accomplish the following:*

>

> *1] track and capture in a log(s) everything this user does upon login including any attempt to su to another user. The log(s) should preferably be stored somewhere other than the user's home directory so that any attempt to hide one's tracks is difficult.*

>

> *2] be alerted when this user logs in. I suppose I can use 'last' for that purpose unless there's a more proactive way to know this.*

>

> *3] Any other strategy you know of that can aid in keeping tabs on the activities of this user.*

>

> *Any documentation you can point me to help gain a better understanding of the issues involved is also appreciated.*

>

> *By the way, the user will login remotely using putty-ssh.*

>

> *TIA*

>

> *VK*

>

>

>

>